



**U.S. Department of Energy
Electricity Advisory Committee Meeting
NRECA Conference Center
Arlington, VA
September 14, 2017**

Summary of Meeting

PARTICIPANTS

EAC:

JOHN ADAMS
Electric Reliability Council of Texas

LANEY BROWN
Concentric Energy Advisors

PAUL HUDSON
Osprey Energy Group

MLADEN KEZUNOVIC
Texas A&M University

JEFF MORRIS
Washington State House of Representatives

ROLF NORDSTROM
Great Plains Institute

PAM SILBERSTEIN
National Rural Electric Cooperative Association

RAMTEEN SIOSHANSI
Ohio State University

DAVID WADE
Electric Power Board of Chattanooga

TOM WEAVER
American Electric Power

DOE:

GIL BINDEWALD
Department of energy

CAITLIN CALLAGHAN
Department of Energy

LOUISE FICKEL

Department of Energy

TRAVIS FISHER

Department of Energy

CATHERINE JEREZA

Department of Energy

HANK KENCHINGTON

Department of Energy

JOYCE KIM

Department of Energy

KEVIN LYNN

Department of Energy

LARRY MANSUETI

Department of Energy

JOHN MCILVAIN

Department of Energy

DAVID MEYER

Department of Energy

MELISSA PAULEY

Department of Energy

MATT ROSENBAUM

Department of Energy

JULIE SMITH

Department of Energy

Speakers, Guests and Members of the Public:

NOHA ABDEL-KARIM

NERC

ANNALEE ARMSTRONG

S&P Global Market Intel

MELODY BALCET
AES

VENKAT BANUNARAYANAN
NRECA

ANTHONY GRIECO
Cisco

STEVE GRIFFITH
NEMA

JOE HENRY
Deloitte

ARTHUR HOUSE
State of Connecticut

CARL IMHOFF
PNNL

BARRY LAWSON
NRECA

DAVID NICOL
University of Illinois at Urbana-Champaign

PAUL PARFORMAK
CRS

THERESA PUGH
Theresa Pugh Consulting

RICHARD RAINES
ORNL

JAMES REILLY
Reilly Associates

JAMIE SHIMEK
PNNL

ALISON SILVERSTEIN

NASPI

BLAKE SOBCZAK
E&E News

WENDY WALLACE
Deloitte

LORNA WISHAM
First Energy

ICF/Support:

CECELIA COFFEY
ICF

LAUREN ILLING
BCS

CHELSEA PELLECCCHIA
ICF

JOSH SMITH
ICF

ANGELA TROY
ICF

YILONG XU
ICF

* * * * *

Panel Session: Cybersecurity

Laney Brown thanked the panelists for participating, Paul Centolella for organizing, and Josh Smith for executing. Ms. Brown gave an overview of the motivations behind the panel, including the Internet of Things panel held at the March 2017 meeting. Ms. Brown introduced the Cybersecurity panelists including: Carl Imhoff, Electric Infrastructure Sector Lead at PNNL; David Nicol, Professor and Director of the Information Trust Institute at University of Illinois at Urbana-Champaign; Anthony Grieco, Senior Director and Trust Strategy Officer at Cisco; and Arthur House, Chief Cybersecurity Risk Officer for the State of Connecticut.

The first panelist, Mr. Imhoff, began by outlining the scope of his presentation, indicating he would first discuss the cyber resilience status of the national power system. Second, Mr. Imhoff planned to introduce Pacific Northwest National Lab (PNNL) and its views of near-term opportunities to improve grid cyber resilience. Third, Mr. Imhoff would frame emerging fundamental opportunities to advance cyber resilience. Finally, he indicated he would suggest several key questions for industry researchers and experts to address.

Mr. Imhoff initially outlined the challenge facing utilities and other grid actors and operators today. He stated that the internet economy is expected to continue to profoundly impact how, and how many, devices interact at the grid edge given that 20 million grid edge devices are expected to be deployed by 2025. The U.S. grid is under constant attack, he added; attacks are increasing, though further details are not fit for discussion in a public forum. Mr. Imhoff elaborated that attackers include foreign governments and that while industry has responded strongly, the response has not been complete and risks still exist.

Mr. Imhoff shared that the 2015 FAST Act designated DOE as lead sector-specific agency for cybersecurity for the energy sector. DOE and the national labs are also uniquely at the nexus of classified intelligence and non-classified utility operational awareness. In addition, as a steward for fundamental science and applications to the power system, as well as connected assets, DOE is a critical place for research and development activities to be conducted. From the national perspective, Mr. Imhoff commented that the U.S. bulk power system is vulnerable as a result of the incomplete implementation of security best practices, among other factors. Limited access to real-time situational awareness and information sharing of cyber threats and vulnerabilities, the growing use of digital systems, and increasing sophistication of threat actors were noted as other factors. Mr. Imhoff suggested yet other benefits result from the power system being able to leverage an interconnected grid; these underlie a need to learn how to get full value out of digital opportunity while simultaneously preserving necessary cybersecurity measures.

Referring to the national cyber innovation landscape, Mr. Imhoff commented that utilities are securing communications and their information technology systems. The largest utilities are leading, followed by mid-size utilities, albeit with more limited resources. Vendors meanwhile are innovating around information technology solutions and tools, but are hindered by the reality that solutions are often proprietary. In addition, Mr. Imhoff shared that the national lab system is conducting fundamental research and specialized testing to support innovation and lead the transition to control systems protection. In addition to PNNL, Sandia National Laboratory (SNL), Oak Ridge National Laboratory (ORNL), Idaho National Laboratory (INL), and Los Alamos National Laboratory (LANL) are key contributors. Mr. Imhoff commented that university partnerships linking fundamental research and workforce development include the University of Illinois, the University of Arkansas, and many other niche academic collaborations that are making advances in the field.

Mr. Imhoff continued his presentation by reviewing several DOE initiatives linked to cyber resilience. First, he noted the research supported by the Cybersecurity for Energy Delivery Systems (CEDS) program under the purview of the Office of Electricity Delivery and Energy Reliability (OE). Mr. Imhoff shared that a Lab Call had been announced the week of the meeting and that progress continued to be made on finalizing the Grid Modernization Multi-Year

Program Plan (MYPP), which includes key recommendations to support cybersecurity activities. In addition, the advanced grid modeling program overseen by OE – which asked the national labs and the Electric Reliability Corporation of Texas (ERCOT) to develop a more compelling tool to understand the risks around cascading outages – is supporting the deployment of a tool to be implemented by the General Electric PLSF community. Mr. Imhoff also described how DOE is helping to plan around the risk of cascading outages in the future. He elaborated, commenting that there is a risk of overemphasizing fixing the cyber components of security since much of the protection response and control tools require a systems approach dealing with all hazards. If cyber is the only focus, risks are created sub-optimal solutions are created, only to be regretted downstream. Mr. Imhoff also provided an overview of the role played by the Advanced Research Projects Agency-Energy (ARPA-E), which has recently explored distributed controls frameworks for resilience to all hazards and developed data and modeling repositories to accelerate innovation. Overall, ARPA-E has supported the designing of better cyber tools and better tools to secure distributed energy markets. Next, the Office of Science within DOE was discussed for its mathematics centers supporting work on advanced control theory, including specifically how the energy industry needs to adapt its tools to secure distributed control devices. In addition, the Office has explored the first grid applications for exascale computing; a program is emerging even though the machines do not yet exist. Mr. Imhoff commented that one benefit of cybersecurity as a sector is that it has brought together various arms of DOE over the last few years to collaborate and produce better solutions. Finally, Mr. Imhoff briefly mentioned an end-use programs initiative under the Office of Energy Efficiency and Renewable Energy (EERE) related to Internet of Things best practices, as well as cybersecurity initiatives under the Office of the Chief Information Officer.

Mr. Imhoff next commented on DOE's outreach and response to industry events. DOE became involved early in information-sharing functions by convening Information Sharing and Analysis Centers (ISACs) and the Cybersecurity Risk Information Sharing Program (CRISP), which both support information sharing, situational awareness, and incident response in both steady state and crisis state scenarios. Mr. Imhoff emphasized that part of preparedness is cyber exercises, but another segment is maturity model self-assessments like the Cybersecurity Capability Maturity Model (C2M2) driven by the North American Electric Reliability Corporation (NERC). Moving to the DOE Grid Modernization Initiative (GMI), Mr. Imhoff highlighted again the MYPP, as well as the recent Lab Call, which yielded \$30 million in awards for the development of more resilient distribution systems. In addition, several GMI initiatives look at new metrics: in addition to affordability and reliability, industry is looking to develop metrics to better measure resilience and flexibility of both grid components and the system as a whole. New valuation tools also are being developed, specifically those capable of measuring how much resilience an area can afford or that stakeholders are willing to fund. Mr. Imhoff emphasized that if the valuation question could not be answered, that new technology will not make it to market. Grid architecture framing, he supplemented, illustrates where increased system risk develops as the trend toward digital systems advances. By examining alternate approaches and considering emerging market concepts, the labs can anticipate accumulated risk. Further, roadmaps for sensing and system observability in the modern grid are critical, he added, as is examining what price points are needed on systems in order to achieve something like time-synchronous system management.

Mr. Imhoff transitioned to focus the next segment of his presentation on a recent white paper published on improving grid cybersecurity. Several recommendations served as conclusions: (1) to implement preventative cyber best-practices for vulnerable mid-sized utilities; (2) to improve near-real-time cybersecurity situational awareness and information-sharing; (3) to secure U.S. electric power system infrastructure in a way that maintains lifecycle integrity; and (4) to examine fundamental research and development projects that ought to be undertaken by the national labs. Mr. Imhoff shared several expected outcomes, should these measures be implemented. First, cybersecurity best practices could be implemented across all utilities. Second, information sharing related to cybersecurity could be improved. Third, risk could be addressed whenever infrastructure is routinely replaced or upgraded – as with grid modernization trends in general. Fourth, foundational research could underlie further industry innovation. Overall, several recommendations were intended to target mid-sized utilities. Mr. Imhoff commented that the largest utilities implemented security best practices more consistently, while the smallest utilities were typically less-attractive targets, while the mid-size utilities tended to be less adequately protected. Overall, securing the grid system component supply chain from product development to acquisition, maintenance, and through retirement would be critical.

Mr. Imhoff also presented a list of emerging fundamental research topics, with an eye toward where the “cyber-resilience research puck” needs to be ten years from now. He emphasized that increased attention needed to be paid to control system-wide, while integrating informational technology (IT) and operational technology (OT) is critical. Modeling and simulation of exascale datasets, with high velocity – which require low latency – would be another significant academic achievement capable of supporting broader private innovation in the future. Other concepts emerging included new methods for system authentication and management, as well as alternative communications network structures. New fundamental grid elements, in turn, could take advantage of new technology and the ability to leverage advanced control theory. In addition, the capabilities of machine learning have grown as computation has advanced so that researchers know better the grid system (and data) limitations. Going forward, a profound opportunity exists for detecting anomalies on large, high-velocity data sets.

In closing thoughts, Mr. Imhoff posited several key questions. These included who pays for resilience and who gets paid for providing resilience, especially since a strong public goods dimension complicates attempts to close risk points. These also include how to incentivize the right behavior to get utilities to a position of cybersecurity resilience. Finally, how can industry and government each continue to improve defenses on both the IT and OT sides. Referring to opportunities in the science and technology realm that enable answering these questions, Mr. Imhoff pointed to high performance computing supporting deep learning for grid analytics. In addition, the ability to construct and model advanced grid architectures for “all hazards” and the ability to leverage valuation tools for cyber resilience to guide investment all will enable more rapid discovery and adoption of cybersecurity best practices.

The second panelist, David Nicol, thanked Mr. Imhoff and suggested that they would be highlighting many of the same points. Dr. Nicol started his presentation by providing context on his own background as director of the Information Trust Institute at the University of Illinois, which has been doing research activities related to power grid cybersecurity since 2004.

The Cyber Resilient Energy Delivery Consortium (CREDC) is the current center that supports projects that move research results into practice. The Information Trust Institute (ITI) also supports the Defense Advanced Research Projects Agency (DARPA) Rapid Attack Detection, Isolation and Characterization (RADICS) program, with a test bed for development. The “DARPA impossible” problem is to develop a framework for evaluating technologies, through exercise-based and other analytic means, noted Dr. Nicol, e.g., modeling the Western interconnect. When discussing disruptive technologies, he suggested the EAC consider the impact of EVs. He noted validation and verification as another key challenge – and difference – between doing the right thing, and doing the right thing right.

Discussing areas needing attention, Dr. Nicol stated that a main area is incentivizing businesses and utilities to choose to invest in new security technologies. In order to do so, however, there is a need to be able to quantify the benefit to purchasers. Quantification could be in terms of risk, but the expensive protection for rare events is a hard sell. Since the classical definition of risk relies on a low probability times a high cost, Dr. Nicol commented that there is a psychological tendency to discount a rare but high consequence event. So, a space where one can address some of these issues is in the development of technologies that advance security, while also adding other kinds of quantifiable benefits. These include monitoring and analysis technologies, which can identify bad, rare events, but also give better constant insight into system behavior in the form of data analytics. Other technologies include those designed to lower maintenance costs, like software-defined networking. Finally, additional areas needing attention include information sharing; CRISP and the Cybersecurity for the Operational Technology Environment (CYOTE) pilot program exist, but participation is limited and other incentives and vehicles for information sharing are necessary.

Protecting crypto-assets involves both raising the bar against intruders and minimizing damage when compromises happen, Dr. Nicol explained. Technology supporting rapid recovery from cyber intrusion includes architectural support like virtualization, intrusion detection, and “usable” response forensics tools. These can all close the gap between knowledge and operation.

Dr. Nicol added that another area needing attention is assessment. Specifically, there is a need for a tool to be able to reason about tradeoffs between good economic reasons to use new technologies and the economic tradeoff of increasing the attack surface. Dr. Nicol suggested that industry players need to be able to assess specific risks; for example, “should we allow someone who is doing maintenance to connect their iPad to my system?” Finally, there is room for improved trust in communications and provenance of digital artifacts. Dr. Nicol asked the assembled group to remember that when Stuxnet happened, a USB was able to represent itself as an encrypted driver because there was only one cryptographic “check” that the system conducted. He provided that story as an example of why methodologies for increased checks, applied dynamically, can bolster cybersecurity. Dr. Nicol concluded his presentation by posing a question to EAC members: how do utilities increase the number of checks made to authenticate system devices without slowing down or compromising the system as a whole?

The third panelist, Anthony Grieco, provided a different perspective on the global conversation around security and IoT from his position helping customers globally think about and act on cybersecurity risk. From his perspective, the game has changed: adversaries’ skill has accelerated

beyond what was experienced or expected in past years. Adversaries are not just attacking providers, but also attacking service providers for BPS operators. Mr. Grieco suggested that adversaries leverage ecosystem attacks, but also interruption of service or exposure of latent risks that are already in the system. He added that attackers use the IT infrastructure as a place to enter and compromise OT operations and infrastructure. Overall, Mr. Grieco commented that consistent use of several “good hygiene” and basic practices could better ensure utilities are not exposing the low-hanging fruit to these adversaries. Related to IoT, digitization and connectivity everywhere have increased latent risks, which include outdated, legacy architectures and infrastructures. As a summary statistic, Mr. Grieco noted that 92% of existing interconnections have known vulnerabilities.

As summary recommendations, Mr. Grieco stated that security has been used as a scare tactic, but that digitization and connectivity trends cannot be reversed. He suggested that industry needs to adapt to the idea that security done properly can be the enabler of success. Utilities in this frame of mind would embrace IoT by investing in architectural approaches to security. As a warning to utility executives, Mr. Grieco cautioned: “If you are not finding ways to train and educate everyone in your organizations about their role in cybersecurity and managing threats, then you’re doing something wrong.” In order to achieve this type of cultural shift, Mr. Grieco added that the expectation needs to be established that security is the responsibility of everyone. He said that greater thought needs to be given about how to make security pervasive, so that security criteria are integrated everywhere. Finally, he indicated that utilities and other stakeholders need to rethink resilience. When considering the fact that destruction of service is a primary goal of adversaries, Mr. Grieco warned that greater thought needs to be given to the criticality of communications: not just how to get the operations back up, but how to restore communications so that bulk system functionality is restored.

The final panelist, Arthur House, began his presentation by outlining that he would draw from his experience in the federal government, as well as his participation in response and recovery efforts from cyber incidents. As an introduction, Mr. House explained that he had worked in both the public and private sectors. In 2012, he left the Office of the Director of National Intelligence (DNI) to serve as chairman of the State of Connecticut’s Public Utilities Regulatory Authority (PURA). When he left, colleagues from FERC and the intelligence community took him aside, Mr. House recounted, to warn that the country has a profound vulnerability to cyberattacks at the state level. These commenters added that regulators at state PUCs are overwhelmed because they do so much for energy, telecommunications, mergers and acquisitions, and other transactions. When Mr. House noted that when he was at the PURA, only four of 200 staff members held security clearances. He concluded that states were not equipped to take on the challenge of cyber resilience.

Mr. House commented that Connecticut sees hurricanes and ice storms and therefore ought to be able to handle them. As a state, Connecticut has never seen a cyberattack. In 2014, the state issued a strategy that Mr. House had developed jointly with utilities. The strategy called for an action plan to assess and take remedial action on cybersecurity. Other innovative efforts to cross-collaborate on cybersecurity included Mr. House’s creation of technical committees, within which conversation could be kept private and through which gas, electric and water utilities could decide when and how to move forward. Mr. House commented on the absence of the

telecommunications industry from these discussions, noting that they saw cooperation in cybersecurity strategizing as a slippery slope to re-regulation.

Of the other three utility sectors, Mr. House shared that three conclusions were reached. First, annual reviews of cybersecurity capacity and the state of defense would be conducted. Second, industry could bring any number of participants to the table, while the state would limit participation to two PURA representatives and two emergency managers. Third, it was determined that sectors could pick their own evaluation metrics; in the end, all four stakeholders selected C2M2. Mr. House offered this anecdote as evidence that it is difficult but possible to change culture. This is the first time in the U.S. that a state has met with utilities to meet in depth and discuss cybersecurity planning. Mr. House said the report – agreed to by all four actors – would come out by the end of the month.

Following the success of his leadership on public-private coordination, Mr. House was asked by Connecticut Governor Malloy to leave the PURA and to serve as chief cybersecurity officer for the state. Last October, Mr. House began his new role with a focus on five areas important to change in the cybersecurity arena: state government, municipal government, higher education, private business, and law enforcement. Mr. House listed several priorities for private business. These include critical infrastructure protection, the defense sector – represented by United Technologies, Pratt & Whitney, and Sikorsky – and the insurance industry. Governor Malloy announced that part of the work outlined for Mr. House would be the development of investigations units capable of conducting cybersecurity investigations and supporting municipal police forces. The answer became “fusion centers,” areas to share intelligence between state, local and federal partners with a focus on crime. More specifically, fusion centers break the intelligence available for basic cybersecurity down to basic police work. Mr. House cited Kansas’s fusion center as an outstanding model, and noted that the state’s utilities provide funding. That said, approaches like Kansas’s have been controversial; detractors suggest it is structurally improper to devolve intelligence to the state level in the private sector. A similar initiative was underway in New England, Mr. House added, but it is too soon to know how successful it will be.

Because Connecticut is the first state to have a strategy and action plan for the PURA – and for the state itself – the state has been working with Ukraine, Armenia, Georgia, Moldova and others to put together better strategies and move forward. Mr. House noted that cybersecurity is a game of offense, since defenses are very restricted, limited, and unable to provide adequate security. He compared the paradigm to the U.S. Navy, which needs to both protect the U.S. from naval invasion from another country, and also to project U.S. naval power around the world. Response and recovery, meanwhile, also goes beyond the realm of the state. In the case of the Colonial pipeline, if the pipeline were knocked out, then products can’t be refined in New Jersey and issues are also created in New York. Gas is even more vulnerable: if key pipelines are knocked out, the effect is mass panic and also the crippling of electricity generation in New England. With a cybersecurity attack, the key is to communicate immediately what is known and unknown. However, Mr. House conveyed that a gap exists between emergency managers and the natural inclination of police not to talk about incidents. Further, he conveyed the primary need to focus on lifesaving and life-sustaining during initial incident response and cautioned that fundamental breakdowns in civil society could occur relatively quickly. Considering a disaster

lasting more than two weeks, Mr. House presented a cascading scenario in which water treatment plants shut down and those who can migrate will leave the area. Lastly, Mr. House indicated he had always seen lots of cooperation from FERC, which supports exchanging information, but noted that there is not much coordination with the federal government until calamity strikes. Other than from FEMA, the provision of emergency services does not typically come from the federal government. Instead, every state has provisions where the management of the emergency (after FEMA leaves) is left in the hands of the state government, including the governor being able to declare martial law and take unilateral action.

EAC Discussion of Cybersecurity

Paul Hudson asked the panelists to comment on how DOE and the National Labs are addressing non-regulated actors, given that distressed independent power producers (IPPs) are attached to the system and microgrid activity is increasing. Mr. Imhoff replied that DOE is engaged with the National Renewable Electric Cooperative Association (NRECA) and the American Public Power Association (APPA), which cover the scope of utility populations. In addition, vendors are engaged in validation efforts in the field. Mr. Imhoff also suggested that the work of industry touches the IPPs. When it comes to microgrids, DOE has substantial engagement with control room development and is working with the states to develop tools to assess, value, and examine investment strategy. Considering distributed resources, Mr. Imhoff suggested there are touchpoints, though these do not connect everywhere. Dr. Nicol suggested thinking about microgrids as one vehicle toward resiliency. He suggested the key question then relates to connecting microgrids to the main grid and to each other. Mr. House added three points. First, microgrids are decentralized, so if the grid goes down, they are more resilient. Second, he raised the discussion in New England about nuclear power, that it is environmental and self-contained. If a pipeline is cut, electricity is still being generated, which supports a security argument for nuclear. In looking at businesses in Connecticut, defense is most resilient. Third, Mr. House reiterated the necessity of careful employee screens. He suggested “need to know” ought to be in effect for those assigned to work on a particular area. An association of approximately 70 defense contractors that exchange threats with each other can provide better communication about cybersecurity threats and risks when they collegially share information. Defense contractors have established this structured way in which the defense industry can receive information from the intelligence community, but Mr. House argued that utilities need to get to this state with communicating critical information as well. Other measures related to personnel include conducting better background checks, beyond checking police records. He also suggested that utilities need to employ more people with a Secret clearance.

Paul Hudson asked the panelists what needs to be done, other than top-down initiatives. He mentioned that the IPP community has been stressed financially and there are significant holes in touching those actors. The vendor community may cross-communicate, but he added that gaps exist there as well. Mr. House replied that for businesses in general – especially with a security dimension – either a cybersecurity audit must be conducted, or some kind of public-private partnership will be necessary. Mr. Grieco commented that the insurance industry is also looking at how they can better address risks. Microgrids create interconnection points, introducing a need to think beyond power connections and into communications connections, as well as risk at these interconnections.

John Adams raised a series of questions. First, to Mr. Imhoff, Mr. Adams asked how industry could bring the IT and OT security processes together. He also asked whether there is a true need for the people operating the grid to know about attacks. Mr. Imhoff replied that examining risks on both the IT and OT sides yields common issues; thus, tools and analytics can work on both sides. In addition, a comprehensive understanding of the enterprise-level risk profile is critical. Mr. House concurred that IT and OT need to be combined. He raised Ukraine as a case study where OT and IT were part of the same cybersecurity system and where operations were disrupted through IT. Dr. Nicol added that even on the IT side, siloing is dangerous. Mr. Adams next asked whether communications between NERC, DOE and the national labs were good enough at the current moment; Mr. Imhoff affirmed they were. Mr. Adams finally asked about the list of fundamental research priorities that Mr. Imhoff had presented. He wondered whether further prioritization could be done, noting the importance of the labs and DOE having a sense of what is most pressing. Mr. Imhoff replied that many systems today reflect today's resilience best practices but fall short of what the system will need five to ten years from now. Dr. Nicol added that current systems are designed for performance, rather than security.

Laney Brown asked, when thinking about the communications perspective, whether systems designed today are starting to factor in these considerations so that they will be able to adapt to future issues. In a highly distributed world, looking at better ways to build communication layers will make the system more secure. Mr. Imhoff suggested that there are considerations of new business models that will allow for greater future flexibility, particularly if regulators can rate-base or allow for cost recovery. Mladen Kezunovic considered the intersections between cybersecurity and physical security. He stated one could bring down a system by using cyber methods to impact physical performance, i.e. cyber infiltration can allow an actor to influence load and destabilize the system. In that area, he suggested the space exists for DOE alone. A second part of Dr. Kezunovic's comment focused on open-source software. He expressed a need to contextualize software for an industry that is not used to it. Dr. Kezunovic asked what the method today is for thinking about how to secure the system and deal with these types of penetrations. Referencing security by design, Dr. Kezunovic commented that the legacy systems, like EMS/ DMS, have been in place for 15-20 years. He indicated that these systems could be leveraged to learn about potential security gaps and for DOE to advance new concepts of security by design. Mr. Grieco echoed Dr. Kezunovic's comment that open-source software is important. Mr. Grieco added that the power sector is not the only one grappling with managing risk. He suggested there could be a real role for the EAC or others regarding procurement: that DOE ought to consider requirements for vendors. Mr. House agreed, adding that both good and bad outcomes result from software being open-source. Regarding the role of DOE, Mr. House disagreed, suggesting DOE can be a resource but does not have a role to play in the states. Dr. Nicol suggested greater attention be given to the combined impacts of IT and OT attacks. He raised the possibility of coordinated attacks in distributed physical locations that disrupt situational awareness and destabilize the system, potentially to a point of destruction. Mr. Imhoff clarified that he might be alluding to the issue of cyber-physical control, in which control and protection need to be connected. Regarding open-source software, Mr. Imhoff characterized it as an early innovation trigger, typically picked up by vendors, but not widely used by utilities beyond the initial stages.

Dr. Kezunovic commented for the record that when he raised recommendations to DOE, he assumed that DOE exists. He clarified that he was not suggesting whether state or federal responsibility should be delegated, but that DOE activities ought to continue, while experiences may be gathered from the state or private environment best practices. Mr. Adams thanked the panel and announced a break.

Presentation: Draft Multiyear Plan for Energy Sector Cybersecurity

Deputy Assistant Secretary Henry Kenchington began his presentation by discussing when, in the previous administration, the National Security Council (NSC) asked “how secure *is* the power grid,” and “it depends” was the accurate answer, which was deemed insufficient. Mr. Kenchington shared that answering that question led to the maturity model, which was designed to help utilities assess their own systems so that there would be a market- and peer-driven way to enhance security. Moving forward to the MYPP, DOE started by working with the energy sector partners as early as 2005. Utilities thought that vendors did not produce secure products, while the vendors replied that the utilities were not willing to pay for security. Mr. Kenchington indicated that from the beginning, the shared responsibility indicated that a public-private partnership could be more effective.

In 2005, an energy sector roadmap was developed as a framework to guide public-private partnerships. The roadmap vision was assembled by several groups, including ERCOT, Edison Electric Institute (EEI), Ergon Refining, NERC, DOE, other pipeline and domestic and international operators, the U.S. Department of Homeland Security (DHS), and Entergy. Mr. Kenchington stated that this roadmap has been used for the last ten to twelve years and is still relevant today, but there is a need to measure performance in goals and milestones.

Currently, Mr. Kenchington noted that 49 DOE technologies contribute to 28 milestones. States are involved, and the collaborative process has led to the commercialization of 30 technologies, which are now in use in all 50 states. The Electric Power Research Institute (EPRI) and the National Electric Sector Cybersecurity Organization Response (NESCOR)—with DOE funding—detailed what security controls are needed to protect the advanced metering infrastructure (AMI) data system. The process developed tools that were not available ten years ago to help design-in security procedures when AMI and other smart data systems are installed. That said, Mr. Kenchington stated that the security landscape has changed: policy, technology, and communications models are more complex. The threat has changed the most; adversaries’ capabilities have grown substantially, especially those attacks targeted at control systems. In addition, the electricity delivery system is evolving to meet customer needs and the changing generation mix, but not evolving adequate cybersecurity protections.

Looking at how much is being invested in cybersecurity, Mr. Kenchington noted that resources are generally a non-value-added service. DOE and others are looking at avoided costs, but at some point stakeholders will not be able to afford all protections. He described the conundrum as an asymmetric ballgame: defenders have to be 100% thorough, but the adversaries only need a

single link click to infiltrate the system. Given the idea that this type of game cannot be won by defenders, Mr. Kenchington communicated the need to change the rules or change the game.

Turning to the process of developing the MYPP, Mr. Kenchington said that in 2015 and 2016 participants started to consider whether the DOE and defense consortia were organized properly. Participants asked whether collaborations were leveraging full capabilities of DOE or focusing on the right priorities. At the end of the review process, which consisted of the national labs conducting an assessment and the private sector tracking comments, the MYPP represents what DOE thinks the Department can do in the next five years in the public-private space. The plan outlines ways in which the energy sector can inform DOE strategy. Today, advanced technologies make it easier and more cost effective to implement security. The MYPP identifies several priorities.

First, Mr. Kenchington explained that a need exists to strengthen today's cyber systems and risk management capabilities, even though system penetrations are inevitable. He shared that comments from both the Electricity Subsector Coordinating Council (ESCC) and the Oil and Natural Gas Subsector Coordinating Council (ONGSCC), as well as the EAC, generally concurred that the focus of the MYPP was on track. Example priorities include promoting enhanced situational awareness and information sharing, enabling real-time machine-to-machine capabilities, and developing risk management tools and guidelines, among others. CRISP, used to identify threat patterns across the electric industry by analyzing real-time traffic using U.S. intelligence capabilities has proved to be a very valuable tool, Mr. Kenchington added. Managed today by the Electricity Subsector Information Sharing and Analysis Center (ISAC), CRISP is one example of advanced tools that enhance threat detection and information sharing. Other prominent tools include the Cyber Analytics Tools and Techniques (CATT) and CYOTE programs. In addition, Mr. Kenchington noted that DOE is working with NRECA and APPA to help support cybersecurity efforts in small- and mid-sized utilities.

Second, the MYPP review process identified a need to develop innovative solutions to secure and harden future systems. One key challenge is coordinating cyber incident response and recovery on the national level. Mr. Kenchington shared that DOE had developed Cyber Response Partnership (CRP) teams, largely to address this issue. Third, the MYPP yielded recommendations to accelerate game-changing research and development of resilient electricity delivery systems. Mr. Kenchington offered the Cybersecurity for Energy Delivery Systems (CEDS) program as an example of one successful approach. At the time of the meeting, over \$240 million had been invested in developing tools and technologies being deployed today by industry. Research and development successes include advanced technologies that he said could both enhance cybersecurity and lower operating costs. For example, software defined networking (SDN) improves security and also saves money. Developed under an SEL-led research partnership, advanced cybersecurity intrusion detection and monitoring for field area networks uses the physics of electric power flow to thwart cyber attacks. Mr. Kenchington shared this as one example of how collaborative defense can leverage the power system itself, given that power flows work according to known physical laws. With new intrusion detection tools, smart grid components in less than 40 milliseconds can determine whether commands will result in an

unstable condition and react by either executing or ignoring commands. Mr. Kenchington said that this type of project highlights the benefit of publicly supported research and development that enables private industry to carry the ball forward, noting that this monitoring tool was in the process of being commercialized by ABB.

Final areas of the MYPP that Mr. Kenchington highlighted included developing strategic cybersecurity core capabilities at the national labs. Each one has other focuses than those presented by Mr. Kenchington, but he identified a specific focus of each that relates to cybersecurity in electricity delivery. All told, DOE awarded \$20 million for twenty new projects to support critical early stage research and development of next-generation tools and technology, as well as to build capacity throughout the energy sector for day-to-day operations like cyber threat information sharing.

EAC Discussion of Multiyear Plan for Energy Sector Cybersecurity

Tom Weaver asked about initial coordination between DOE and the U.S. Department of Homeland Security (DHS) regarding cybersecurity. Mr. Weaver gave an example of DHS developing seven steps for cybersecurity. Relative to the questions that came out this year after Ukraine, he asked what evaluations could be used internally to take actions to close gaps. Mr. Kenchington replied that following attacks in Ukraine, DOE, the electricity sector ISAC, and DHS put together a team to go abroad. As a result, through the ISAC, the team developed a use case and conducted training exercises. From a higher level, they worked with the subsector coordinating councils to communicate and coordinate through the national infrastructure protection model.

John Adams complimented Mr. Kenchington's and DOE's ability to plant seeds for cybersecurity protection. Mr. Kenchington replied that DOE is interested in return on investment and spending the least money to have the most impact of improving the security of the whole sector.

Mr. Adams shared a summary of the EAC's comments on the draft MYPP. He gave credit to Paul Centolella who led the Smart Grid Subcommittee in gathering comments and compiling feedback. Mr. Centolella wanted to point out that threats to the power delivery system are asymmetric and dynamic, and thus that non-linear ability is critical. Since the grid is fundamentally an open system, changes in demand can interrupt system operations. Mr. Adams also highlighted the Subcommittee's findings that system integration needs to be protected, especially because of grid interdependencies with natural gas pipelines. Overall, the EAC recommendations highlighted that efficient grid operation is dependent on real-time visibility and communications. Combined attacks on the grid and communication systems have a cumulative effect. Therefore, the Subcommittee recommended that greater attention be devoted to geographic dispersion of critical assets that leaves the system vulnerable.

Other comments included that cybersecurity expertise is limited in the utility workforce. In addition, utilities are dependent upon purchasing technology that comes through a global supply chain, which contributed to uncertain material sourcing. Given that industrial control systems have their infrastructure built over 50-100 years, most systems were not designed with

cybersecurity in mind. The Subcommittee recognized that, with legacy material still in service, damage to some equipment can take months to years to replace. With responsibility for its upkeep split between 3,300 electric utilities, including those that have limited available resources, the education of capable technicians is an issue of critical importance. Citing Equifax as an example, Mr. Adams commented that commercial entities responsible for protection are not always those that will bear the brunt of an attack. With regard to electricity, since oversight of security is split among many levels of regulatory entities' jurisdictions, the FAST Act – which gave DOE the responsibility to protect and restore the reliability of the electric system in an emergency – could serve as a resource to DOE. Mr. Adams opened the floor for suggestions of what more the EAC should be doing, if anything. No comments were offered.

Presentation: DOE Staff Report on Electricity Markets and Reliability

Travis Fisher, Senior Advisor to the DOE Office of Electricity Delivery and Energy Reliability, provided a presentation on the DOE Staff Report on Electricity Markets and Reliability. As background, Mr. Fisher reminded the group that Secretary Perry had requested a grid study in April 2017. Each question addressed in the memo could have been its own staff report, as the memo asked staff to examine: (a) the evolution of wholesale electricity markets, which Mr. Fisher noted was covered in Section 5; (b) compensation for reliability and resilience in the wholesale electricity and capacity markets, covered in Section 4; and (c) causes of premature baseload power plant retirements, covered in Section 3. Mr. Fisher gave a brief overview of the process of developing the report and reiterated the framework. He offered special thanks to Alison Silverstein for driving the bus on the content side, especially while he was leading the forward-facing effort. He indicated that seven national labs participated in developing inputs for the report, in addition to expert contributions from FERC staff and DOE leadership and staff. Mr. Fisher personally thanked David Meyer for his guidance and credited the Office of Energy Policy and Systems Analysis (EPSA) for developing a template process and format when the Quadrennial Energy Review (QER) 1.1 and 1.2 reports were produced.

Mr. Fisher shared that the selection of the report's fifteen-year period of review included several important trends in the energy industry, but was driven by the guidance of the U.S. Energy Information Administration (EIA) that the most recent fifteen years had the highest data integrity. Trends included during this time period included the beginning of merchant generation competing in centrally organized markets, the shale revolution, and the transition from steady demand growth due to electrification to flat demand growth driven by energy efficiency and net metering. He also touched on the importance of defining key terms, including several ways that stakeholders define "premature retirement," since it is an inherently subjective term that the DOE staff chose not to define.

Mr. Fisher noted several key findings of the report. These included that the primary drivers of baseload plant retirements were the decline in gas prices, low load growth, the enforcement of environmental regulations, and increased penetration of variable renewable energy sources. Among these, however, gas prices were the single most impactful trend. On the reliability and

resilience side, the report found that reliability of the bulk power system is adequate today. Markets recognize and compensate reliability only to some extent; however, in wholesale electricity markets, changing circumstances are challenging efficient pricing. These factors include negative pricing, as well as missing money – i.e., markets do not currently value all economic benefits of electricity provision, which extend to include local jobs, economic development, and even national security. Mr. Fisher commented that one underlying principle of the study was that energy pricing is not just a marginal cost-driven environment anymore. In addition, state policy is a layer on top of pure least cost approach.

Mr. Fisher turned to discussing Section 3 of the report, which focuses on power plant retirements. He shared that the report considered tranches of retirements, which were each prompted by specific regulatory deadlines like those established by the Mercury and Air Toxics Standards (MATS). In addition, since gas-fired power plants are becoming more efficient, plants are using less fuel to generate the same kilowatt-hours, just as natural gas supply in the country continues to increase due to fracking and other horizontal drilling technologies. Mr. Fisher commented that electricity demand and economic growth began decoupling, beginning around 2005, and that changing policy and market conditions have made the adjustment to that trend challenging. Compliance with environmental regulations imposes additional economic challenges. Finally, he shared that although variable renewable energy (VRE) penetration is rising, according to research from the Lawrence Berkeley National Lab (LBNL) existing data do not suggest a correlation between VRE penetration and thermal plant retirements. Mr. Adams posed a question: ERCOT has a reliability adder on top of its wholesale electricity prices, but given that the market does not oversee a capacity market, and given that VREs have a different capacity value anyway, he asked whether different market approaches – like energy versus capacity versus reliability adders – are discussed in the report. Mr. Fisher answered that they were, in Sections 4 and 5, with the capacity value question addressed in Section 4 and the markets piece in Section 5.

Mr. Fisher next addressed reliability. He began by sharing several key findings. A diverse portfolio of generation resources and well-planned transmission investments was determined to be critical to meeting regional reliability and resilience objectives. In addition, the study concluded that the central challenge of integrating VRE is managing its effect on grid operations and planning. Finally, there are tradeoffs between multiple desirable attributes for the electric grid. A more reliable and resilient system may be more costly than the least-cost system. From the perspective of the North American Electric Reliability Corporation (NERC), fuel security and reliability come at a cost. An affordable grid is not the same as a resilient grid. Dr. Kezunovic asked whether, when the team was communicating with NERC, they adopted NERC's definition of reliability and resilience, given that there are many angles to each. Mr. Fisher answered that NERC itself somewhat borrows definitions of reliability and resilience from others, adding that he has heard the question a lot – on the difference between reliability and resilience. He suggested that the difference was defined by findings in the report: one can have a very reliable grid that is not resilient. For example, an all-gas grid with firm contracts is reliable, but not resilient if power generation relies on a single pipeline to deliver that gas. Dr. Kezunovic

offered a response that U.S. infrastructure is relatively old, and Mr. Fisher answered that reliability can be split into two parts: the operational piece and the resource adequacy piece. To the resilience question, he noted that the fact that a clear definition has not been developed only supports the imperative at the regional transmission operator (RTO) and FERC level to define terms. Dr. Kezunovic asked a third question: if one examines outages on the grid, are they going up in terms of duration and frequency, or going down. Mr. Fisher commented that the answer could be the subject of yet another deep dive. The only major outages recently on the bulk power system have been in 2003. Most other outages of focus in the report are on the distribution level. Bulk power outage statistics were not necessarily beyond the scope of this report, but the report looks at distribution-level outages in depth in this report, while bulk-level outages are well known.

Other issues related to reliability that the report examined included changing net load shapes and the definitions of reliability from industry and regulatory stakeholders. Regarding net load shapes, RTO/ ISOs are integrating growing levels of VRE, which shift the time of peak load. These resources also introduce more hourly and intra-hourly variability. When talking about flexibility of the system, generators need to meet a shakier net load overall. Borrowing from NERC's reports, Mr. Fisher shared that the study concluded that reliability is adequate. That said, more analysis is required on changing needs for electric reliability services in a future with increasing VRE levels and decreasing rotating mass-based inertia. That said, capacity may be more flexible in the future, given demand has become increasingly flexible with the advent of demand response and other programs. According to PJM, solar and storage are complementary in the types of resource adequacy they provide. Mr. Fisher noted that, as an example, if the focus is on capability and flexibility, then storage has everything needed and nuclear has nearly nothing. But if fuel assurance is the priority, then nuclear does very well. Therefore, the grid not only needs to include a diverse set of resources, but planners need to be conscious about the technology pairings as well.

Mr. Fisher next contrasted reliability with resilience. As the fuel mix changed, more focus was placed on generation because it has seen the most change; however, that trend leads perhaps to over-emphasizing generation, as examined in Appendix A of the report. In reality, greater fuel diversity doesn't always mean greater system reliability or resilience. A PJM simulation, for example, showed that when subjected to a polar vortex event, only 34 of the 98 portfolios which were classified as desirable in terms of reliability were also resilient. Mr. Fisher conveyed the conclusion that diversity should not be a focus for its own sake, but instead for the benefits provided by that diversity. Dr. Kezunovic asked whether the study parsed distributed versus centralized generation characteristics and Mr. Fisher answered that it did not. Other resilience topics in the report included the growing interdependence between electricity and gas and the ability to withstand and recover from extreme weather events. Recent stories about medically dependent facilities highlighted the importance of electricity.

With regard to wholesale electricity markets, Mr. Fisher noted his FERC background and shared that several regions have gone the capacity route. PJM, for example, determined that as low marginal cost units are increasing, the energy revenue for a plant will decline; however, the

capacity price could cover missing money to compensate for fixed costs. In ERCOT, price caps were removed and only an energy price with an operating demand curve price adder was left. Now, wholesale markets are changing their dispatch. The study concluded that low-cost natural gas and subsidized VRE significantly flatten supply curves. Mr. Fisher highlighted that in 2011 coal-fired generation was cheaper than gas, but that today a complete mix of coal and gas generators is distributed along the same cost curve. He added that, in the absence of transmission constraints, relying on price spikes to drive the missing money solution is unreliable. Mr. Fisher also briefly addressed the issue of negative pricing in wholesale markets, suggesting that broadly the trend is not a reason for panic, but nuclear operators face a severe challenge. He also covered issues related to affordability, including price-setting at the locational marginal price and examining various solutions to achieve affordable electricity delivery down to the distribution level.

Mr. Fisher shared several policy recommendations and areas for further research introduced by the study. The report recommended that DOE: (1) Support industry efforts and focus research and development to enhance system resilience; (2) Accelerate and reduce costs for relicensing and permitting of generation facilities; (3) Facilitate programs for workforce development; (4) Prioritize energy dominance and Executive Order 13783 directives; and (5) Increase coordination of electric and natural gas industries. The report recommended that FERC both expedite efforts to reform energy price formation and value essential reliability services. The report suggested that the EPA ought to consider regulations that impact the existing fleet. When discussing areas for further research, Mr. Fisher shared that stakeholders may prefer a shift away from designed transmission in favor of a market-based approach. The transformation of the electricity delivery system could be guided by focusing on achieving reliability and resilience goals. Overall, research areas were divided into four buckets: market structure and pricing, reliability and resilience, cost and affordability, and regulatory issues. Mr. Fisher concluded his presentation and took questions.

EAC Discussion of DOE Staff Report on Electricity Markets and Reliability

Jeff Morris shared concerns expressed by system operators that the view of the distribution service model represented in the paper could erode the fundamental utility business model at the distribution level, and demand drop-off could lead to cascading failure up to the high-voltage system. He criticized not accounting for the evolving utility business model, suggesting that in evaluating retirements in state-regulated utilities, great change is expected throughout the next two decades. Rep. Morris also commented that the Work Product being produced by the Power Delivery Subcommittee on the Transmission-Distribution interface could be critically important in highlighting these gaps in research and development on the federal side. Rep. Morris finally advocated for consideration of customer-driven changes on the distribution side. Mr. Fisher agreed, sharing that he had received similar feedback from California stakeholders. He commented that DOE and others need to figure out a way to be proactive regarding expected changes and flexible regarding unexpected changes. Overall, he echoed the critical importance of figuring out pricing issues and getting both energy and capacity prices “right.”

John Adams asked Mr. Fisher what can be done in the present to make the grid more resilient. Mr. Fisher answered that the specifics are a policy call, but the standard to be met is the pressing question and that there are several areas where improvements are needed. Mr. Adams thanked Mr. Fisher for his participation and moved to the next agenda item.

EAC Smart Grid Subcommittee Update

Laney Brown provided an overview of the Subcommittee and its statutory basis to advise DOE coming from the Energy Independence and Security Act of 2007. She highlighted that the Subcommittee has focused on cybersecurity throughout 2017. In March, the Subcommittee hosted a panel on the Internet of Things (IoT) at the full EAC Meeting. Then in June of 2017, the Subcommittee discussed cybersecurity issues related to IoT and the power grid, including hearing input from Carol Hawk and Hank Kenchington. Ms. Brown updated the full EAC that the Subcommittee recently completed feedback on the draft MYPP of DOE and had also sponsored the panel on cybersecurity that spoke earlier during this same meeting. For potential further consideration, Ms. Brown added that the Smart Grid Subcommittee was considering greater focus on cybersecurity and the IoT, both through evaluating the information provided in the recent panel and through building off of feedback provided on the MYPP. In addition, infrastructure investment in the grid could be a key focus of the Subcommittee going forward, including either examining how to facilitate most economically valuable investments or examining how to maintain U.S. leadership in the development of smart technologies for the power grid.

EAC Power Delivery Subcommittee Update

John Adams provided a Power Delivery Subcommittee update, noting that the Subcommittee has no statutory obligation to provide specific work products. Regarding current work, Mr. Adams gave an overview of the work product examining DOE work on the Transmission-Distribution Interface (TDI), as increasing amounts of DERs are added to the grid. The intent of the work product he described is to examine differing conditions across different regulatory and physical paradigms. Speaking to methodology, Mr. Adams explained how the Subcommittee had developed a list of regions and selected interviewees from each region who are experts in their specific geographic area and could speak to challenges surrounding the integrated planning and operation of the transmission and distribution systems. He added that the Subcommittee planned to present a Work Product for approval in February. In addition, Mr. Adams updated the EAC that the Subcommittee was working to define its next work product, but that Subcommittee members had preferred to defer selection of the next work product until the next Subcommittee call.

EAC Energy Storage Subcommittee Update

Ramteen Sioshansi, Chair of the Energy Storage Subcommittee, updated the full EAC that the Subcommittee was currently developing four Work Products, which were at various stages.

The first Work Product focuses on energy storage for reliability and resilience, under the basic premise that energy storage has a potential role to play in addressing reliability and resilience needs of electricity service at the same time as it could serve some of the system's more routine energy needs. The Work Product is intended to survey a potential use case and builds off of a day-long workshop on this topic held during the June 2017 EAC meeting. Dr. Sioshansi noted one temporary setback: of the three primary people who were working on this Work Product, two have come off of the EAC since the June meeting, but both Ake Almgren and Janice Lin have volunteered to continue providing support to Laney Brown, who will be the lead EAC member in developing the product. Since the workshop material, notes, and transcript have been compiled and the Work Product is being drafted by the working group for Subcommittee review, the anticipated completion date is the February 2018 EAC Meeting.

The second Work Product examines alternate forms of energy storage. Since the EAC has typically focused on electricity storage, this Work Product evaluates where that focus should be expanded to include a wider range of energy storage technologies. The purpose of this work is to provide definitional and scoping information to the DOE on alternate energy storage technologies. Dr. Sioshansi indicated that follow-on work products would provide more detail, but that an initial scoping memo had been developed by Jim Lazar that highlights alternate energy storage technologies, and had been circulated and was being revised based on feedback.

The third Work Product evaluates Rate, Tariff & Regulatory Design for Energy Storage. Dr. Sioshansi indicated he had taken the lead on the project himself, with assistance from former EAC members Tom Sloan and Ralph Masiello. As background, Dr. Sioshansi shared that traditionally resources are either considered assets or market participants, but that energy storage does not fit neatly into these buckets, as it is a unique power system. He added that the purpose of the Work Product is to define the problem and survey what has been implemented at the federal and state level—as well as in RTO/ISO markets and at the utility level—to address issues. Dr. Sioshansi added that the final goal of the Work Product would be recommendations to DOE regarding what it can do to facilitate addressing these issues going forward. In terms of progress, a working group had been formed and had developed an initial list of topics, but now needed to narrow the scope. Dr. Sioshansi also indicated that the group would schedule a conversation with DOE to see how the list should be expanded to provide a high-value Work Product.

Dr. Sioshansi introduced the fourth and final Work Product, the 2018 Biennial Storage Review, as one of the few EAC Work Products that is statutorily required, via the Energy Independence and Security Act of 2007 (EISA 2007), Title VI, Section 641 (e) (5), which mandates that the Council shall assess every two years the performance of the DOE in meeting the goals of the plans developed under paragraph four of the Act. In 2016, the two-year and five-year required reports were combined. So far, Dr. Sioshansi shared that no progress had been made on the Work Product because the Subcommittee was awaiting a response from DOE to the 2016 review document. Dr. Sioshansi supported continuing to wait for the DOE response to ensure that the

scope of the 2018 review would be most useful. Mr. Adams asked whether it was reasonable to consider deferring one of the Work Products to a later time. Dr. Sioshansi replied that deferral was an option, but because different Members were taking different leads, these Work Products may either happen concurrently or defer themselves. Ms. Brown added that the Work Products are not only being completed by different teams, but are also at different stages of development, with the first two much further advanced, the fourth upcoming, and the third only in the preliminary stage.

Public Comments

Theresa Pugh suggested that future meetings might consider significant localized infrastructure impacts. As a lobbyist and gas industry consultant, she also raised the possibility of using liquefied natural gas storage and other forms of gas storage in states where the geology is ill-suited for traditional natural gas storage.

Wrap-up and Adjourn September 2017 Meeting of the EAC

John Adams called for any final comments from members. He asked whether there were any objections to sending informal letters of thanks to the leadership that had recently rolled off the Committee on behalf of the Committee members. Hearing none, Mr. Adams said he would issue those letters.

Mr. Adams also commented that he thought the meeting was very worthwhile and that he hopes that further discussions will follow on next steps. He called for new members to sign up for Subcommittees and thanked all members for attending and participating. He adjourned the meeting at 12:50 PM.

Respectfully Submitted and Certified as Accurate,



John Adams
ERCOT
Acting Chair
DOE Electricity Advisory Committee

02/20/2018

Date



Ramteen Sioshansi
The Ohio State University
Acting Vice-Chair
DOE Electricity Advisory Committee

2/20/2018

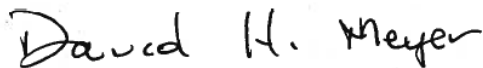
Date



Matthew Rosenbaum
Office of Electricity
Designated Federal Official
DOE Electricity Advisory Committee

02/20/2018

Date



David Meyer
Office of Electricity
DOE Electricity Advisory Committee

02/20/2018

Date